IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 17, 2019, accepted August 30, 2019, date of publication September 3, 2019, date of current version September 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2939272

Enhancing Physical Layer Security of DF Buffer-Aided Relay Networks With Small Buffer Sizes

CHEN WEI[1], ZHIFU YIN[2], WENDONG YANG[1], AND YUEMING CAI[1]
[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]First Information Sustainment Brigade of Eastern Theater Command Army, Fuzhou 350000, China

Corresponding author: Wendong Yang (ywd1110@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61771487 and Grant 61371122.

ABSTRACT In this paper, we propose a novel max-weight secure link selection (MWSLS) scheme to enhance physical layer security of decode-and-forward (DF) buffer-aided relay networks. The MWSLS scheme can select the link with the largest weight among all secure and available source-to-relay and relay-to-destination links. By modeling the dynamic buffer state transitions as a Markov chain, we derive the closed-form expressions of the secrecy outage probability, the secrecy diversity gain, the average secrecy throughput and the end to end delay, which provide a comprehensive and effective way to evaluate the impacts of different parameters on the secrecy performance. The results of this paper reveal that: 1) For the case with small buffer sizes, a significant enhancement on the secrecy outage performance can be observed compared with the popular max-link secure link selection (MLSLS) scheme. 2) When $L \geq 3$, the secrecy diversity gain of the system can achieve $2M$, while the MLSLS scheme achieves the same secrecy diversity gain only when $L \to \infty$ (where M denotes the number of relays and L is the buffer size). 3) The MWSLS scheme outperforms the MLSLS scheme in terms of the average secrecy throughput and the end to end delay in the low signal-to-noise ratio (SNR) regime, and obtain the same performance as the latter in the high SNR regime.

INDEX TERMS Buffer-aided relay, physical layer security, max-weight secure link selection, secrecy performance.

I. INTRODUCTION

Relay technique is seen as a promising way to extend the coverage of wireless networks and provides a variety of performance enhancements, which has attracted enormous research interest [1]–[3]. However, in conventional cooperative relay networks, the half-duplex relay must follow a prefixed schedule for data transmission or reception [4]. That is to say, the data packet is received by the selected relay in the first time slot, and then forwarded to the destination in the second time slot, which results in the consequence that the best channel cannot be utilized in a fast-fading environment, therefore limiting the performance of the network.

Recently, a number of studies demonstrate that the performance of conventional relay networks can be further enhanced by equipping data buffers at relay nodes, because it can take full advantage of the additional transmission flexibility provided by the buffers [5], [6]. At present, various buffer-aided relaying schemes have been proposed in [7]–[10]. Among all the existing buffer-aided relay selection schemes, the max-link relay selection scheme is of particular interest [9]. The main idea of the max-link scheme is to select the link with the best channel quality among all source-to-relay and relay-to-destination links in each time slot, which can achieve the diversity gain of $2M$ when the buffer sizes are large enough (M is the number of relays). However, the diversity gain reduces to M when the buffer sizes are small. Motivated by this, the author in [10] proposed a new relay selection scheme, called the ''max-weight'' scheme, which relaxes the requirement of the link quality and considers the buffer status as the dominant metric for relay selection. As shown in [10], the optimal diversity gain of $2M$ can also be achieved even with small buffer sizes.

The associate editor coordinating the review of this manuscript and approving it for publication was Liang Yang.

Furthermore, due to the open and dynamic nature of the wireless channels, the security of data transmission is becoming a crucial issue for the wireless networks [11], [12]. The traditional way to protect the data transmission against eavesdropping is utilizing the cryptographic algorithms in the upper layers [13], which cannot guarantee the security of the system absolutely and can be decrypted easily with the rapid development of the computer technology. As an alternative, physical layer security has been proposed as a promising method to secure the wireless networks by utilizing the characteristics of the wireless channels [14]–[17]. Because buffer-aided relay networks are also faced with the challenge above, a great amount of researches have been carried on physical layer security of buffer-aided relay networks [18]–[25]. In [18], a link selection scheme that adapts the reception and transmission time slots based on the channel quality was proposed to improve the transmission efficiency and security of the two-hop buffer-aided relay network. The authors in [19] proposed a joint optimal link selection and power control scheme to maximize the average secrecy throughput while considering a single-relay scenario. For multi-relay scenarios, a max-ratio relay selection scheme was proposed in [20], which can improve the security of transmission in buffer-aided decode-and-forward (DF) wireless networks by selecting the relay with the largest signal to eavesdropper channel gain ratio. Later, the work in [21] considered the buffer-aided relay with amplify and forward (AF) mode, and the results indicated that higher level security can be achieved compared to AF relay networks without buffers. In [22], the authors introduced cognitive radio (CR) to buffer-aided relay networks, and investigated the secrecy performance for DF cognitive radio networks with finite buffers. The work in [23] took the scenario of relays with multiple antennas into account and adopted maximal ratio combining (MRC) and maximal ratio transmission (MRT) protocol at the relay nodes to enhance the secrecy performance of the system. In [24], the system model of [23] was extended to a multiple-input multiple-output (MIMO) scenario, and a buffer-aided joint transmit antenna and relay selection (JTARS) scheme based on the main channel was proposed to enhance the secrecy performance of the considered system. Additionally, to further improve the secrecy performance, the opportunistic relay and jammer scheme was employed, which can enhance the physical layer security of the multiuser MIMO buffer-aided relay networks by utilizing artificial noise [25].

However, it is easily observed that the link or relay selection schemes adopted by most literatures above consider the link quality as the dominant selection metric, while there are no strict requirements for the buffer status. Accordingly, the buffer of the corresponding relay with good link quality tends to be full or empty easily, which may result in the decrease of the available links.

Motivated by these observations, we propose a novel max-weight secure link selection (MWSLS) scheme to improve the secrecy performance of the dual-hop DF buffer-aided relay networks. For comparison, the secrecy analysis of the max-link secure link selection (MLSLS) scheme is also presented. The main contributions of this paper are summarized as follows:

1) We propose a novel secure link selection scheme to enhance physical layer security of DF buffer-aided relay networks which considers the buffer status as the dominant selection metric rather than the link quality considered by most existing literatures.
2) We derive the exact expressions of the secrecy outage probability, the average secrecy throughput and the end to end delay in closed-form respectively by utilizing the Markov chain theory. These derived analytical expressions enable us to evaluate the impacts of different parameters such as the buffer size, the number of relays on the secrecy performance.
3) To obtain deeper insights, we also derive the asymptotic secrecy outage probability in the high signal-to-noise ratio (SNR) regime, from which the secrecy diversity gain can be further derived. Specifically, the optimal secrecy diversity gain of $2M$ can be achieved for the MWSLS scheme as long as $L \geq 3$, while only when $L \to \infty$, the MLSLS scheme can achieve the same secrecy diversity.

The remainder of the paper is organized as follows. In Section II, the system model and proposed secure link selection scheme are introduced. Section III investigates the secrecy outage probability of the system. Analysis of other performance metrics are provided in Section IV. Section V presents simulation results and discussions. Finally, we summarize the conclusions of this paper in Section VI.

Notation: In this paper, we use lower-case and upper-case boldface symbols to denote the vectors and matrices respectively. $\|\cdot\|$ and $(\cdot)^T$ denote the Euclidean or L_2 vector norm and the transpose operation. The cumulative distribution function (CDF) and the probability density function (PDF) of the random variable γ are denoted as $F_\gamma(\cdot)$ and $f_\gamma(\cdot)$ respectively.

II. SYSTEM MODEL AND PROPOSED SECURE LINK SELECTION SCHEME

A. SYSTEM MODEL

We consider a dual-hop multi-relay network consisting of one source node S, one destination node D, M half-duplex DF relays $\{R_k\}_{k=1}^{M}$ and one eavesdropper E, as illustrated in Fig. 1. In the network, all the nodes are equipped with a single antenna except E, which is equipped with N_E antennas. All the channels suffer from the quasi-static flat Rayleigh fading so that the channel coefficients remain unchanged during the coherent time of the channels [26]. It is assumed that direct link between S and D is unavailable due to significant path loss and shadowing effects caused by obstacles [20]. Furthermore, each relay is equipped with a data buffer B_k of finite size L and the data packets in the buffer obey the "first-in-first-out" rule.

Throughout this paper, we define h_{AB} as the channel coefficient of link $A \to B$, which is a complex Gaussian random

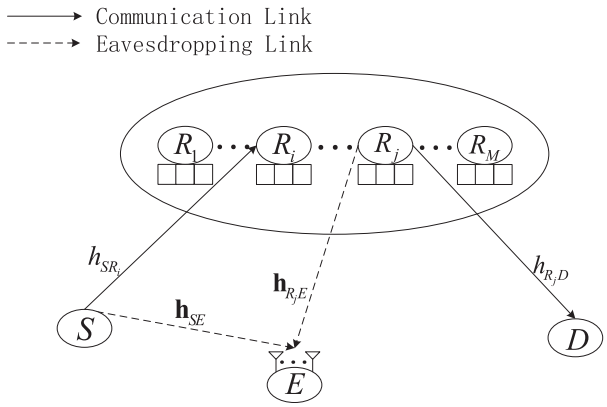

FIGURE 1. System model.

variable with zero mean and variance λ_{AB}. Hence, the channel gain $|h_{AB}|^2$ is an exponentially distributed random variable with mean λ_{AB}. In addition, we assume that the main and wiretap channels are independent and nonidentical. More specifically, the main channels are assumed to be independent and identically distributed (i.i.d), i.e., $\lambda_{SR_i} = \lambda_{R_jD}$. On the other hand, the wiretap channels are also i.i.d, i.e., $\lambda_{SE} = \lambda_{R_jE}$.

B. PROPOSED SECURE LINK SELECTION SCHEME

In order to delve into the buffer-aided secure link selection scheme, we first model the number of the data packets in each buffer as a state. Thus $s_n = [\varphi_n(1), \varphi_n(2), \cdots, \varphi_n(M)]^T$ denotes the n-th state of the possible states, where $\varphi_n(k) \in \{0, 1, \cdots, L\}$ $(1 \le k \le M)$ represents the number of data packets in buffer B_k at state s_n.

It's worth noting that under state s_n, the relay R_k can receive or transmit data packets if the corresponding buffer B_k is not full or not empty, i.e., $\varphi_n(k) \ne L$ or $\varphi_n(k) \ne 0$. Therefore, $\phi_{1,n}(k) = 1$ (or $\phi_{2,n}(k) = 1$) denotes the case that the relay R_k can be selected for reception (or transmission) at state s_n in the first (or second) hop. That is to say, the corresponding link is available in this case. On the contrary, $\phi_{1,n}(k) = 0$ (or $\phi_{2,n}(k) = 0$) represents the case that the relay R_k cannot be utilized to receive (or transmit) data packets in the first (or second) hop, which means that the corresponding link is unavailable. Based on this, we have

$$\phi_{1,n}(k) = \begin{cases} 1, & \varphi_n(k) \ne L \\ 0, & \varphi_n(k) = L \end{cases} \tag{1}$$

and

$$\phi_{2,n}(k) = \begin{cases} 1, & \varphi_n(k) \ne 0 \\ 0, & \varphi_n(k) = 0 \end{cases} \tag{2}$$

After that, the number of available links in the first and second hops at state s_n are respectively given by

$$M_{1,n} = \sum_{k=1}^{M} \phi_{1,n}(k), \tag{3}$$

$$M_{2,n} = \sum_{k=1}^{M} \phi_{2,n}(k). \tag{4}$$

Besides, to make the subsequent secrecy analysis tractable, we denote the achievable secrecy rate of the first hop as [27]

$$C_{SRE} = \left[\log_2\left(1 + \gamma_{SR_k}\right) - \log_2\left(1 + \gamma_{SE}\right)\right]^+ \tag{5}$$

where $\gamma_{SR_k} = P_S \left|h_{SR_k}\right|^2 / \sigma^2$ and $\gamma_{SE} = P_S \left\|\mathbf{h}_{SE}\right\|^2 / \sigma^2$ denote the received SNR at R_k and E respectively, $\mathbf{h}_{SE}$ represents the $N_E \times 1$ channel vector between S and E. In addition, P_S is the transmit power of S, σ^2 is the variance of the additive white Gaussian noise (AWGN), and $[x]^+ = \max\{0, x\}$.

Similarly, the achievable secrecy rate of the second hop is given by

$$C_{RDE} = \left[\log_2\left(1 + \gamma_{R_kD}\right) - \log_2\left(1 + \gamma_{R_kE}\right)\right]^+ \tag{6}$$

where $\gamma_{R_kD} = P_R \left|h_{R_kD}\right|^2 / \sigma^2$ and $\gamma_{R_kE} = P_R \left\|\mathbf{h}_{R_kE}\right\|^2 / \sigma^2$ represent the received SNR at D and E. Similarly, $\mathbf{h}_{R_kE}$ denotes the channel vector between R_k and E, P_R is the transmit power of R_k.

Then, before introducing the proposed scheme, i.e., the MWSLS scheme, we first review the popular MLSLS scheme in the following.

Inspired by [9], the MLSLS scheme is taking the secrecy constraints into consideration, which can be mathematically expressed as

$$R^*_{MLSLS} = \underset{k \in [1:M]}{\arg\max} \left\{ \bigcup_{\varphi(k) \ne L} \gamma_{SR_k}, \bigcup_{\varphi(k) \ne 0} \gamma_{R_kD} \right\} \tag{7}$$

The MLSLS scheme can increase the achievable secrecy rate by enlarging the difference between the quality of the main channels and the eavesdropper's channels. However, the impact of the buffer status is not taken into account in the MLSLS scheme, hence the relay with good link quality may be selected frequently, and its buffer tends to be empty or full easily.

Therefore, the proposed MWSLS scheme is designed from the perspective of the buffer status, which relaxes the requirement of channel quality. Note that this novel scheme is also inspired by [10], but different from [10], the physical layer security in a cooperative buffer-aided relay network is explored simultaneously. Furthermore, the secrecy outage is defined as the event that the achievable secrecy rate is less than the predefined secrecy rate R_s. That is to say, if the achievable secrecy rate greater than R_s, the corresponding link is regarded as secure and available. The main idea of the MWSLS scheme is that the higher priority is given to the buffer status, while the link quality only meets the requirement that it is not in secrecy outage. More specifically, we first define the weight of link $S \to R_k$ $(R_k \to D)$ as $L - \varphi(k)$ $(\varphi(k))$ according to the current buffer status and then the weight is allocated to the corresponding link. Next, this scheme selects the link with the largest weight among all secure and available links. From this proposed scheme, we can observe that the relay with the least packets

in its buffer is selected at the first hop and the relay with most packets in its buffer is selected at the second hop. The MWSLS scheme can be described as

$$R^*_{MWSLS} = \arg\max_{k\in[1:M]} \left\{ \bigcup_{\varphi(k)\neq L,\, \frac{1+\gamma_{SR_k}}{1+\gamma_{SE}}\geq\gamma_{th}} \{L-\varphi(k)\}, \bigcup_{\varphi(k)\neq 0,\, \frac{1+\gamma_{R_kD}}{1+\gamma_{R_kE}}\geq\gamma_{th}} \{\varphi(k)\} \right\} \quad (8)$$

where $\gamma_{th} \triangleq 2^{2R_s}$ is the secrecy outage threshold. Note that the exponential term is "$2R_s$" due to that the whole transmission process is divided into two time slots.

C. COMPARISON OF CSI REQUIREMENT AND COMPLEXITY

In this part, we provide a comparison of CSI requirement and complexity between the MWSLS and MLSLS schemes. According to the analysis above, we find that the CSI of the main channel, i.e., h_{SR_k} and h_{R_kD}, are needed for both schemes. Besides, the CSI of the wiretap channel is also needed during the process of link selection under the MWSLS scheme. Hence, in this paper, we assume that the eavesdropper is normally an active member of the network, and the eavesdropper's CSI can be obtained. Based on this, the MWSLS scheme has a higher complexity than the MLSLS scheme due to a large amount of feedback overhead during the acquisition of eavesdropper's CSI, which is the limitation of this scheme. From the analysis above, we can observe that the MWSLS improves the security of the system at the cost of increasing the system complexity compared with the MLSLS scheme.

III. SECRECY OUTAGE ANALYSIS

In this section, we analyze the secrecy outage performance of the DF buffer-aided relay networks under the MWSLS scheme. Considering all of the possible states, the secrecy outage probability of the system can be given by [9]

$$P_{out}(\gamma_{th}) = \sum_{n=1}^{N} \pi_n P_{out,n}(\gamma_{th}), \quad (9)$$

where $N = (L+1)^M$ is the total number of states, π_n and $P_{out,n}(\gamma_{th})$ denote the stationary distribution probability and the secrecy outage probability at state s_n respectively.

A. THE SECRECY OUTAGE PROBABILITY AT STATE s_n: $P_{out,n}(\gamma_{th})$

Given a state s_n, we derive the exact and asymptotic secrecy outage probability in this subsection. To make the following analysis tractable, we assume that the variance of the AWGN is $\sigma^2 = 1$, and then we define $\gamma_{SR'_{M_{1,n}}E} = \left(1+\gamma_{SR'_{M_{1,n}}}\right)/(1+\gamma_{SE})$ and $\gamma_{R''_{M_{2,n}}DE} = \left(1+\gamma_{R''_{M_{2,n}}D}\right)/\left(1+\gamma_{R''_{M_{2,n}}E}\right)$, where $\gamma_{SR'_{M_{1,n}}} = P_S\left|h_{SR'_{M_{1,n}}}\right|^2$, $\left|h_{SR'_{M_{1,n}}}\right|^2 = \max_{\varphi_n(k)\neq L}\left\{\left|h_{SR_k}\right|^2\right\}$ and $\gamma_{R''_{M_{2,n}}D} = P_R\left|h_{R''_{M_{2,n}}D}\right|^2$, $\left|h_{R''_{M_{2,n}}D}\right|^2 = \max_{\varphi_n(k)\neq 0}\left\{\left|h_{R_kD}\right|^2\right\}$. Moreover, we also denote $\bar{\gamma}_{SR} = E\left(\gamma_{SR_k}\right)$, $\bar{\gamma}_{RD} = E\left(\gamma_{R_kD}\right)$, $\bar{\gamma}_{SE} = E\left(\gamma_{SE}\right)$ and $\bar{\gamma}_{RE} = E\left(\gamma_{R_kE}\right)$. Then, according to [24], the secrecy outage probability at state s_n is given by

$$P_{out,n}(\gamma_{th}) = F_{\gamma_{SR'_{M_{1,n}}E}}(\gamma_{th}) \cdot F_{\gamma_{R''_{M_{2,n}}DE}}(\gamma_{th}) \quad (10)$$

Theorem: The exact and asymptotic CDF of $\gamma_{SR'_{M_{1,n}}E}$ are respectively given by

$$F_{\gamma_{SR'_{M_{1,n}}E}}(x) = \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} (-1)^s e^{-\frac{s(x-1)}{\bar{\gamma}_{SR}}} \times \left(\frac{\bar{\gamma}_{SR}}{\bar{\gamma}_{SR}+sx\bar{\gamma}_{SE}}\right)^{N_E} \quad (11)$$

and

$$F_{\gamma_{SR'_{M_{1,n}}E}}(x) \overset{\bar{\gamma}_{SR}\to\infty}{\approx} \left(\frac{x}{\bar{\gamma}_{SR}}\right)^{M_{1,n}} \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} \times \left(\frac{x-1}{x}\right)^{M_{1,n}-s} \frac{(s+N_E-1)!}{(N_E-1)!} \bar{\gamma}_{SE}^{s} \quad (12)$$

Proof: See Appendix A. ∎

Note that if we make substitution of the parameters, i.e., $M_{1,n} \to M_{2,n}$, $P_S \to P_R$, $\bar{\gamma}_{SR} \to \bar{\gamma}_{RD}$, we can derive the exact and asymptotic CDF of $\gamma_{R''_{M_{2,n}}DE}$. On the other hand, to make the following analysis tractable, we define $\bar{\gamma} = \bar{\gamma}_{SR} = \bar{\gamma}_{RD}$ as the average SNR, and $\bar{\gamma}_E = \bar{\gamma}_{SE} = \bar{\gamma}_{RE}$ be fixed.

Furthermore, the exact and asymptotic CDF of $\gamma_{SR'_{M_{1,n}}E}$ can be regarded as the function of $M_{1,n}$, we denote it as $P_1\left(M_{1,n}\right)$ and $P_1^{\infty}\left(M_{1,n}\right)$ respectively. Similarly, the exact and asymptotic CDF of $\gamma_{R''_{M_{2,n}}DE}$ can be expressed as $P_2\left(M_{2,n}\right)$ and $P_2^{\infty}\left(M_{2,n}\right)$. Recalling the assumption of a symmetric channel scenario we considered, hence we have $P_1(\delta) = P_2(\delta) = P(\delta)$, $P_1^{\infty}(\delta) = P_2^{\infty}(\delta) = P^{\infty}(\delta)$, where δ is the number of available links.

B. THE STATIONARY PROBABILITY AT STATE s_n: π_n

Now, we focus on the stationary probability $\boldsymbol{\pi}$. Firstly, we divide the sets of states which can be transferred from state s_n within one step into two sets, denoted as Ω_n^1 and Ω_n^2. Specifically, if the source-to-relay link is selected, the buffer state will transfer from state s_n to one of the states in Ω_n^1. On the other hand, if the relay-to-destination link is chosen, the buffer state will transfer to another state in Ω_n^2.

According to [9], we denote $\mathbf{A} \in \mathbb{R}^{N\times N}$ as the state transition matrix of the Markov chain, where the entry $\mathbf{A}_{v,n} = \Pr[T(t+1) = s_v \,|\, T(t) = s_n]$ is the transition probability to move from state s_n at time slot t to state s_v at time slot $t+1$, s_v represents one of the elements in Ω_n^1 or Ω_n^2.

Based on the secure link selection scheme, we find that the buffer state remains unchanged if the data packet is not successfully transmitted to the correspond node. That is to say, the secrecy outage event occurs. On the other hand, when $s_v \in \Omega_n^1$ or $s_v \in \Omega_n^2$, it means that the corresponding transmission is successful.

From these observations, the entry of the state transition matrix is given by

$$\mathbf{A}_{v,n} = \begin{cases} P_{out,n}(\gamma_{th}), & s_v = s_n \\ P_n^{SR_k}, & s_v \in \Omega_n^1 \\ P_n^{R_kD}, & s_v \in \Omega_n^2 \\ 0, & else \end{cases} \tag{13}$$

where $P_n^{SR_k}$ and $P_n^{R_kD}$ denote the probability that the link of $S \to R_k$ and $R_k \to D$ are selected respectively.

Now, we proceed with the derivation of $P_n^{SR_k}$ and $P_n^{R_kD}$.

Firstly, according to the MWSLS scheme, the weight vector at state s_n is given by

$$\mathbf{w}_n = \left[w_n^1, w_n^2, \cdots, w_n^{2M}\right], \tag{14}$$

where $w_n^k = L - \varphi_n(k)$, $w_n^{M+k} = \varphi_n(k) (1 \le k \le M)$ represent the weight of $S \to R_k$ and $R_k \to D$ respectively. Given a weight $w_n^\theta \ne 0 (1 \le \theta \le 2M)$, we define $N_{n,\theta}^{lar,1} = \sum_{k=1}^{M} \varpi_1\left(w_n^k\right)$ and $N_{n,\theta}^{lar,2} = \sum_{k=M+1}^{2M} \varpi_1\left(w_n^k\right)$ as the number of $S \to R_k$ and $R_k \to D$ links whose weight are lager than w_n^θ, respectively, where $\varpi_1\left(w_n^k\right) = \begin{cases} 1, & w_n^k > w_n^\theta \\ 0, & else \end{cases}$. Similarly, let us denote $N_{n,\theta}^{eq,1} = \sum_{k=1}^{M} \varpi_2\left(w_n^k\right)$ and $N_{n,\theta}^{eq,2} = \sum_{k=M+1}^{2M} \varpi_2\left(w_n^k\right)$ as the number of $S \to R_k$ and $R_k \to D$ links whose weight are equal to w_n^θ respectively, where $\varpi_2\left(w_n^k\right) = \begin{cases} 1, & w_n^k = w_n^\theta \\ 0, & else \end{cases}$.

To obtain the transition probability at state s_n, three events are defined as follows.

$$E_n = \left\{\text{A link with the weight of } w_n^k \text{ is selected}\right\} \tag{15}$$

$$E_n^1 = \left\{\text{All the } N_{n,\theta}^{lar,1} + N_{n,\theta}^{lar,2} \text{ links with larger weights than } w_n^k \text{ are not secure and unavailable}\right\} \tag{16}$$

$$E_n^2 = \left\{\text{At least one of the } N_{n,\theta}^{eq,1} + N_{n,\theta}^{eq,2} \text{ links with the weight of } w_n^k \text{ is secure and available}\right\} \tag{17}$$

According to the MWSLS scheme, we find that the event E_n occurs only if the event E_n^1 and E_n^2 occur simultaneously. Note that the event E_n^1 and E_n^2 are independent, hence we have $E_n = E_n^1 \cap E_n^2$, and the probability of the event E_n is

$$\begin{aligned} \Pr(E_n) &= \Pr\left(E_n^1\right) \cap \Pr\left(E_n^2\right) \\ &= P\left(N_{n,\theta}^{lar,1}\right) P\left(N_{n,\theta}^{lar,2}\right) \left[1 - P\left(N_{n,\theta}^{eq,1}\right) P\left(N_{n,\theta}^{eq,2}\right)\right] \end{aligned} \tag{18}$$

If $1 \le (\theta = k) \le M$, the $S \to R_k$ link is chosen, and the probability $P_n^{SR_k}$ is given by

$$P_n^{SR_k} = \frac{P\left(N_{n,k}^{lar,1}\right) P\left(N_{n,k}^{lar,2}\right) \left[1 - P\left(N_{n,k}^{eq,1}\right) P\left(N_{n,k}^{eq,2}\right)\right]}{N_{n,k}^{eq,1} + N_{n,k}^{eq,2}} \tag{19}$$

where the coefficient is $1/(N_{n,k}^{eq,1} + N_{n,k}^{eq,2})$ because the probability to select a certain link among all the links with equal weights is the same and equal as $1/(N_{n,k}^{eq,1} + N_{n,k}^{eq,2})$.

Following the similar analysis, if $M+1 \le (\theta = M+k) \le 2M$, the corresponding probability $P_n^{R_kD}$ can be expressed as

$$P_n^{R_kD} = \frac{P\left(N_{n,M+k}^{lar,1}\right) P\left(N_{n,M+k}^{lar,2}\right) \left[1 - P\left(N_{n,M+k}^{eq,1}\right) P\left(N_{n,M+k}^{eq,2}\right)\right]}{N_{n,M+k}^{eq,1} + N_{n,M+k}^{eq,2}} \tag{20}$$

With these observations, we can obtain the stationary distribution probability vector, which is given by [9]

$$\boldsymbol{\pi} = (\mathbf{A} - \mathbf{I} + \mathbf{Q})^{-1} \mathbf{b} \tag{21}$$

where $\boldsymbol{\pi} = [\boldsymbol{\pi}_1, \boldsymbol{\pi}_2 \cdots, \boldsymbol{\pi}_N]^T$, $\mathbf{b} = (1, 1, \cdots, 1)^T$, $\mathbf{I}$ is the identity matrix and $\mathbf{Q}$ is the all-ones matrix.

Therefore, the exact and asymptotic closed-form expression of the secrecy outage probability can be derived, and in order to obtain more insights, we will proceed with the investigation of the secrecy diversity gain, the average secrecy throughput and the delay in the following section.

IV. OTHER PERFORMANCE METRIC ANALYSIS

In this section, the secrecy diversity gain, the average secrecy throughput and the end-to-end delay of the buffer-aided relay network are investigated, which can provide a comprehensive and effective method to evaluate the secrecy performance of the system.

A. SECRECY DIVERSITY GAIN

To indicate the achieved secrecy diversity gain visually for the buffer-aided relay network with small buffer sizes, the special case such as $L = 2$ is investigated by following similar analysis as [10].

Firstly, we divide the N states into $M+1$ state sets S_β $(0 \le \beta \le M)$, which can be given by

$$S_\beta = \left\{ \bigcup_{n\in[1:N]} s_n : \sum_{k=1}^{M} \varpi\left(\varphi_n(k)\right) = \beta \right\} \tag{22}$$

where S_β represents the set which has β empty or full buffers, and $\varpi\left(\varphi_n\left(k\right)\right) = \begin{cases} 1, & \varphi_n\left(k\right) = L \text{ or } 0 \\ 0, & else \end{cases}$. Given a state set S_β, note that there are $2M-\beta$ available links. More specifically, we assume that there are β_1 unavailable links in the first hop and β_2 unavailable links in the second hop, where $\beta_1+\beta_2=\beta$. Hence the secrecy outage probability can be represented as

$$P_{out} = \sum_{\beta=0}^{M} P\left(M-\beta_1\right)P\left(M-\beta_2\right)\tilde{\pi}_\beta \tag{23}$$

where $\tilde{\pi}_\beta$ denotes the stationary probability if the current state being in the state set S_β.

Then, denoting $\tilde{\mathbf{A}}$ as the "state set" transition probability matrix and following similar analysis as [10], we can obtain the entry of $\tilde{\mathbf{A}}$ for the special case $L=2$, which is given by

$$\tilde{\mathbf{A}}_{\alpha,\beta} = \begin{cases} P\left(M-\beta_1\right)P\left(M-\beta_2\right), & \alpha=\beta \\ 1-P\left(\beta_1\right)P\left(\beta_2\right), & \alpha=\beta-1 \\ P\left(\beta_1\right)P\left(\beta_2\right)-P\left(M-\beta_1\right)P\left(M-\beta_2\right), & \alpha=\beta+1 \\ 0, & else \end{cases} \tag{24}$$

where $0\le\alpha\le M$. Since the Markov chain we consider is irreducible and aperiodic, we have $\tilde{\mathbf{A}}\tilde{\boldsymbol{\pi}}=\tilde{\boldsymbol{\pi}}$. According to this equation, we can obtain the relationship between $\tilde{\pi}_\beta$ and $\tilde{\pi}_0$, which can be written as

$$\tilde{\pi}_\beta = \tilde{\pi}_0 \prod_{l=0}^{\beta-1} \frac{P\left(l_1\right)P\left(l_2\right)-P\left(M-l_1\right)P\left(M-l_2\right)}{1-P\left(l_1\right)P\left(l_2+1\right)} \tag{25}$$

where $1\le\beta\le M$ and $l_1+l_2=l$.

Since $\sum_{\beta=0}^{M}\tilde{\pi}_\beta=1$ always holds, therefore we can obtain

$$\tilde{\pi}_0 = \frac{1}{1+\sum_{m=1}^{M}\left[\prod_{l=0}^{m-1}\frac{P(l_1)P(l_2)-P(M-l_1)P(M-l_2)}{1-P(l_1)P(l_2+1)}\right]} \tag{26}$$

$$\tilde{\pi}_\beta = \frac{\prod_{l=0}^{\beta-1}\frac{P(l_1)P(l_2)-P(M-l_1)P(M-l_2)}{1-P(l_1)P(l_2+1)}}{1+\sum_{m=1}^{M}\left[\prod_{l=0}^{m-1}\frac{P(l_1)P(l_2)-P(M-l_1)P(M-l_2)}{1-P(l_1)P(l_2+1)}\right]}, \quad 1\le\beta\le M \tag{27}$$

According to [28], the secrecy diversity gain can be defined as

$$d = -\lim_{\bar{\gamma}\to\infty}\frac{\log_2 P_{out}}{\log_2\bar{\gamma}} \tag{28}$$

Hence the asymptotic secrecy outage probability is given by

$$P_{out}^{\infty} \overset{\bar{\gamma}\to\infty}{\approx} \sum_{\beta=0}^{M} P^{\infty}\left(M-\beta_1\right)P^{\infty}\left(M-\beta_2\right)\tilde{\pi}_\beta^{\infty} \tag{29}$$

Corollary 1: The asymptotic stationary probability $\tilde{\boldsymbol{\pi}}^{\infty}$ can be expressed as

$$\begin{aligned}\tilde{\pi}_0^{\infty} &\approx \frac{1}{2} \\ \tilde{\pi}_{\beta,\beta\ge1}^{\infty} &\approx \frac{\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\frac{\beta(\beta-1)}{2}}\prod_{l=0}^{\beta-1}\left[\sum_{s=0}^{l}\binom{l}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{l-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]}{2}\end{aligned} \tag{30}$$

Proof: See Appendix B. ■

Substituting (30) into (29), the asymptotic secrecy outage probability can be rewritten as (31), shown at the top of the next page.

It is worth noting that when $\beta=1$ or 2, $(\gamma_{th}/\bar{\gamma})^{2M-1}$ is a lower order term compared to other terms. That is to say, it dominates the whole expression while other terms are approximated as 0. Hence when $L=2$, the secrecy diversity gain of $d=2M-1$ can be obtained.

Next, resorting to [10, eq. (24)], we can derive the results for the case $L=3$.

Corollary 2: The asymptotic stationary probability $\tilde{\boldsymbol{\pi}}^{\infty}$ for the $L=3$ case can be expressed as

$$\tilde{\pi}_\beta^{\infty} \approx \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\beta M}\left[\sum_{s=0}^{M}\binom{M}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]^{\beta} \tag{32}$$

Proof: See Appendix C. ■

Similarly, the asymptotic secrecy outage probability with for the $L=3$ case is given by (33), shown at the top of the next page.

Form the expression above, we find that the corresponding term $(\gamma_{th}/\bar{\gamma})^{(\beta+2)M-\beta}$ dominates the expression (33) when $\beta=0$, which results in that the secrecy diversity gain is equal to $2M$. That is to say, for the case $L=3$, the system can achieve the optimal secrecy diversity gain, hence when $L>3$, the same optimal secrecy diversity gain of $2M$ can also be achieved.

Furthermore, for the case $L=1$, we can easily obtain that the secrecy diversity gain is equal to M. Based on the analysis above, the secrecy diversity gain of the MWSLS scheme can be expressed as

$$d_{MWSLS} = \begin{cases} M, & L=1 \\ 2M-1, & L=2 \\ 2M, & L\ge3 \end{cases} \tag{34}$$

Remark: The MLSLS scheme can achieve the optimal secrecy diversity gain of $2M$ under the scenario $L\to\infty$. On the other hand, when L is finite and small, the secrecy diversity gain of the MLSLS scheme is reduced to M because it is limited by the states with full or empty buffers. Motivated by this, the MWSLS scheme is designed to prevent the buffer

$$P_{out}^{\infty} \overset{\bar{\gamma}\to\infty}{\approx} \frac{1}{2}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{2M} \sum_{s_1}^{M}\sum_{s_2}^{M}\binom{M}{s_1}\binom{M}{s_2}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{2M-s_1-s_2} \frac{(s_1+N_E-1)!}{(N_E-1)!}\frac{(s_2+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s_1+s_2} + \frac{1}{2}\sum_{\beta=1}^{M}\left[\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\frac{\beta(\beta-3)}{2}+2M}\prod_{l=0}^{\beta-1}\left[\sum_{s=0}^{l}\binom{l}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{l-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]\sum_{s_1}^{M-\beta_1}\sum_{s_2}^{M-\beta_2}\binom{M-\beta_1}{s_1} \times \binom{M-\beta_2}{s_2}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{2M-\beta-s_1-s_2}\frac{(s_1+N_E-1)!}{(N_E-1)!}\frac{(s_2+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s_1+s_2}\right] \tag{31}$$

$$P_{out}^{\infty} \overset{\bar{\gamma}\to\infty}{\approx} \sum_{\beta=0}^{M}\left[\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{(\beta+2)M-\beta}\left[\sum_{s=0}^{M}\binom{M}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]^{\beta}\sum_{s_1}^{M-\beta_1}\sum_{s_2}^{M-\beta_2}\binom{M-\beta_1}{s_1}\binom{M-\beta_2}{s_2} \times \left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{2M-\beta-s_1-s_2}\frac{(s_1+N_E-1)!}{(N_E-1)!}\frac{(s_2+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s_1+s_2}\right] \tag{33}$$

from being full or empty effectively, therefore it can achieve the optimal secrecy diversity gain of $2M$ even when L is small.

B. AVERAGE SECRECY THROUGHPUT AND END TO END DELAY

This subsection investigates the average secrecy throughput and the end to end delay of the system under the MWSLS scheme.

The average secrecy throughput represents the average rate of the transmitted information which is kept confidential to the eavesdropper. Due to the fact that the system is delay-limited, resorting to [29] and [30], the average secrecy throughput is given by

$$\bar{T} = \bar{R}R_s\left(1 - P_{out}\left(\gamma_{th}\right)\right) \tag{35}$$

where $\bar{R}$ denotes the average data transmission rate of the system, and we have $\bar{R} = \frac{1}{2}$ due to that it takes two time slots for every packet to reach the destination node.

Then we will proceed with the analysis of the end to end delay. In the buffer-aided relay network, the end to end delay of a data packet is the time interval between the packet leaves the source node and reaches the destination node, which can be expressed as

$$\bar{D}_{total} = \bar{D}_S + \bar{D}_R \tag{36}$$

where $\bar{D}_S$ and $\bar{D}_R$ denote the average delay at the source node and the relay nodes respectively. We find that $\bar{D}_S = 1$ always holds owing to that only one time slot is taken when every packet transmits from the source node to the relay node. Furthermore, since the probabilities to choose a certain relay R_k among all M relays are the same, hence we have $\bar{D}_{R_k} = \bar{D}_R$ and $\bar{T}_k = \bar{T}/M$, where $\bar{D}_{R_k}$ and $\bar{T}_k$ represent the delay and the average secrecy throughput at relay R_k respectively.

On the other hand, given a state s_n, denoting the queuing length in the buffer of relay R_k as $\varphi_n(k)$, hence the average queuing length at R_k if considering all states is given by

$$\bar{Q}_k = \sum_{n=1}^{N}\pi_n\varphi_n(k) \tag{37}$$

According to the Little's law [28], the average packet delay at relay R_k can be expressed as

$$\bar{D}_{R_k} = \frac{\bar{Q}_k}{\bar{T}_k} \tag{38}$$

Finally, invoking the corresponding expression above, the average end to end delay can be given by

$$\bar{D}_{total} = 1 + \frac{2M\sum_{n=1}^{N}\pi_n\varphi_n(k)}{R_s\left(1 - P_{out}\left(\gamma_{th}\right)\right)} \tag{39}$$

V. SIMULATION ANALYSIS

In this section, we present comparison simulation results for the secrecy performance of the MWSLS scheme and the MLSLS scheme to verify the theoretical analysis in the previous sections. Without loss of generality, the transmit power of all links are normalized to unity and the predefined secrecy rate is set as $R_s = 1$ bit/s/Hz. As indicated in these figures, the analytical results are in exact agreement with the Monte Carlo simulations which corroborates the accuracy of the theoretical analysis.

Fig. 2 illustrates the secrecy outage probability versus the average SNR $\bar{\gamma}$ for the proposed MWSLS scheme with different number of relays and buffer sizes. As indicated in this figure, the secrecy outage probability is decreased with the increase of M and L. This is intuitive since increasing M or L provides additional secrecy diversity gain. More specifically, for the case $M = 1$, we can see that the secrecy diversity gains of $L = 1, 2, 3$ are 1, 1, 2 respectively. While for the case $M = 2$, the secrecy diversity gains of $L = 1, 2, 3$ increase to 2, 3, 4, which verified the correctness of the theoretical analysis

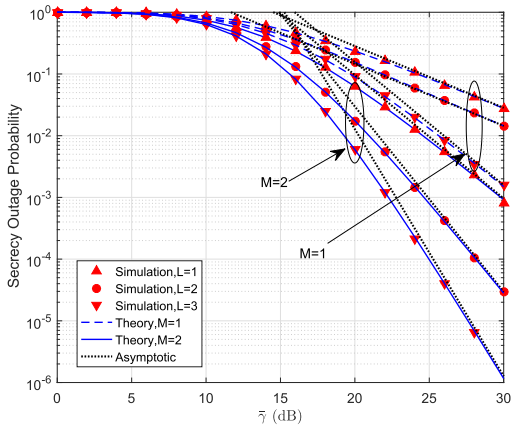

FIGURE 2. Secrecy outage probability vs. the average SNR $\bar{\gamma}$ for the proposed MWSLS scheme when $M = 1, 2$, $L = 1, 2, 3$, $N_E = 2$, $\bar{\gamma}_E = 5$dB.

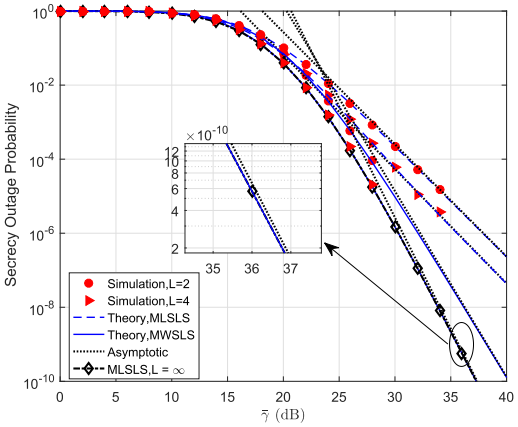

FIGURE 3. Secrecy outage probability vs. the average SNR $\bar{\gamma}$ for different secure link selection schemes when $M = 3$, $L = 2, 4$, $N_E = 2$, $\bar{\gamma}_E = 10$dB.

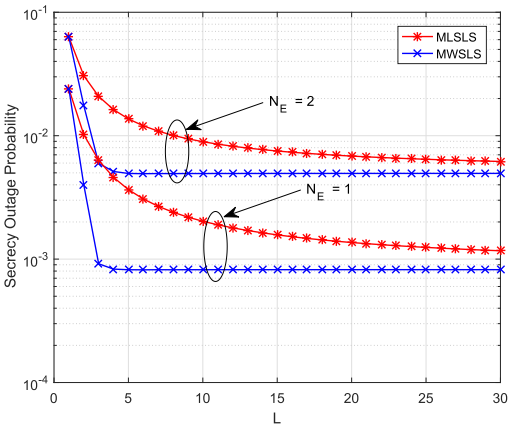

FIGURE 4. Secrecy outage probability vs. the buffer size L for different secure link selection schemes when $M = 2$, $N_E = 1, 2$, $\bar{\gamma} = 20$dB, $\bar{\gamma}_E = 5$dB.

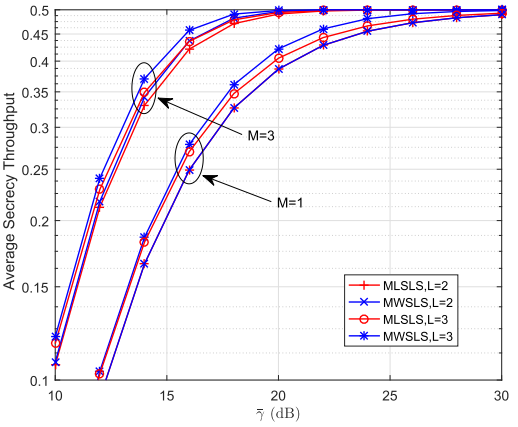

FIGURE 5. Average secrecy throughput vs. the average SNR $\bar{\gamma}$ for different secure link selection schemes when $M = 1, 3$, $L = 2, 3$, $N_E = 3$, $\bar{\gamma}_E = 5$dB.

about the secrecy diversity gain of the proposed MWSLS scheme.

Fig. 3 plots the secrecy outage probability versus the average SNR $\bar{\gamma}$ for the proposed MWSLS scheme and the MLSLS scheme with different buffer sizes. It is observed that the MWSLS scheme outperforms the MLSLS scheme significantly when the buffer sizes are small. That is due to the fact that the former can provides higher secrecy diversity than the latter. To be specific, the MWSLS scheme can achieve the secrecy diversity gains of 5 and 6 when $L = 2, 4$ respectively. However, for the MLSLS scheme, the secrecy diversity gain reduces to 3 for both $L = 2$ and $L = 4$ cases. Moreover, we can find that when the buffer sizes are small, the MWSLS scheme can achieve the same secrecy diversity gain as the MLSLS scheme with infinite buffer sizes, which further indicates the distinct advantage of the proposed MWSLS scheme on the secrecy diversity gain.

Fig. 4 shows the secrecy outage probability versus the buffer size L for the proposed MWSLS scheme and the MLSLS scheme. As can be seen, regardless of the secure link selection scheme, the secrecy outage probability decreases with the increase of the buffer size until the performance floor occurs. Furthermore, it is intuitively observed that the MWSLS scheme can achieve the secrecy performance floor with small buffer sizes, while the MLSLS scheme needs to satisfy the requirement of the long enough buffer sizes, which is because the optimal secrecy diversity gain of $2M$ can be achieved for the MWSLS scheme when $L \geq 3$.

Fig. 5 presents the average secrecy throughput versus the average SNR $\bar{\gamma}$ for the proposed MWSLS scheme and the MLSLS scheme with different number of relays. It is shown that with the increase of the average SNR $\bar{\gamma}$, the average secrecy throughput is increased until it converges to a relatively fixed value $\frac{R_s}{2}$, since the process of the packet transmission takes two time slots. We note that the MWSLS scheme degenerates to the MLSLS scheme when $M = 1, L = 2$. This is because the state transition matrix of MWSLS is the same as that of MLSLS and then the same secrecy performance can be achieved under this special scenario. Furthermore, we can also observe that the proposed MWSLS scheme outperforms the MLSLS scheme in terms of the average secrecy throughput, which matches the analysis in (35).

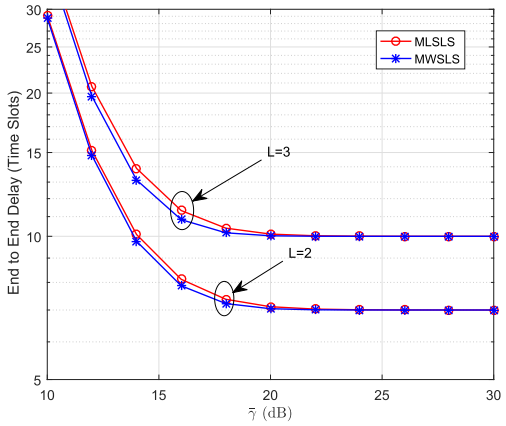

FIGURE 6. End to end delay vs. the average SNR $\bar{\gamma}$ for different secure link selection schemes when $M = 3$, $L = 2, 3$, $N_E = 3$, $\bar{\gamma}_E = 5$dB.

Fig. 6 compares the end to end delay versus the average SNR $\bar{\gamma}$ between the two secure link selection schemes. As shown in this figure, for the two schemes, the end to end delay are both decreased with $\bar{\gamma}$ and approach a lower bound $1+ML/R_s$ when $\bar{\gamma}$ is sufficiently large. Despite this, the lower delay can be obtained using the proposed MWSLS scheme when $\bar{\gamma}$ is not large enough.

VI. CONCLUSION

This paper proposes a novel MWSLS scheme to enhance physical layer security of the considered system by giving higher priority to the buffer status to avoid the event of buffers to be full or empty occurring. We derive the closed-form expressions of the secrecy outage probability, the secrecy diversity, the average secrecy throughput and the end to end delay by modeling the evolution of the buffer status as a Markov chain. The impacts of different system parameters on the secrecy performance is investigated by comparing with the MLSLS scheme. Our findings suggest that for the case with small buffer sizes, the MWSLS scheme can provide a significant secrecy performance boost by comparisons with the MLSLS scheme. In particular, the former achieves the optimal secrecy diversity gain of $2M$ so long as $L \geq 3$, while the latter must require $L \to \infty$ to achieve the same secrecy diversity gain. These results provide useful insights for designing the cooperative buffer-aided relay networks in the presence of an multi-antenna eavesdropper, and this work could be extended to cognitive cooperative or internet of things scenarios in the future.

APPENDIX A

Let us define $X = \left|h_{SR'_{M_{1,n}}}\right|^2$, $Y = \|\mathbf{h}_{SE}\|^2$, according to the order statistic, the exact CDF of $\gamma_{SR'_{M_{1,n}}E}$ can be expressed as

$$\begin{aligned} F_{\gamma_{SR'_{M_{1,n}}E}}(x) &= \Pr\left(\frac{1+P_S X}{1+P_S Y} < x\right) \\ &= \int_0^\infty F_X\left(\frac{x-1}{P_S} + xy\right) f_Y(y)\, dy \end{aligned} \tag{40}$$

According to the secure link selection scheme, the exact CDF of X is given by

$$F_X(x) = \left(1 - e^{-\frac{P_S x}{\bar{\gamma}_{SR}}}\right)^{M_{1,n}}, \tag{41}$$

On the other hand, when $\bar{\gamma} \to \infty$, with the help of $e^x \approx 1 + x\ (x \to 0)$, the corresponding asymptotic CDF of X can be expressed as

$$F_X(x) \overset{\bar{\gamma}\to\infty}{\approx} \left(\frac{P_S x}{\bar{\gamma}_{SR}}\right)^{M_{1,n}} \tag{42}$$

The PDF of Y can be presented as [31]

$$f_Y(y) = \left(\frac{P_S}{\bar{\gamma}_{SE}}\right)^{N_E} \frac{y^{N_E-1} e^{-\frac{P_S y}{\bar{\gamma}_{SE}}}}{(N_E-1)!} \tag{43}$$

Then we substitute (41) and (43) into (40), the exact CDF of the $\gamma_{SR'_{M_{1,n}}E}$ can be easily derived with the help of binomial theorem. Following the similar approach, the desired expression of the asymptotic CDF can be obtained after some simple mathematical manipulations.

APPENDIX B

When $\bar{\gamma} \to \infty$, invoking the asymptotic secrecy outage probability, we have, (44) and (45), as shown at the bottom of this page.

It is obvious that when $m = 1$, the corresponding term is always equal to 1. While $m > 1$, the corresponding term is approximated as 0 when $\bar{\gamma} \to \infty$, hence the denominator of (44) and (45) are equal to 2. To this end, the desired results in **Corollary 1** can be derived.

$$\tilde{\pi}_0^\infty = \frac{1}{1+\sum_{m=1}^{M}\left[\prod_{l=0}^{m-1}\frac{P^\infty(l_1)P^\infty(l_2)-P^\infty(M-l_1)P^\infty(M-l_2)}{1-P^\infty(l_1)P^\infty(l_2+1)}\right]} \approx \frac{1}{1+\sum_{m=1}^{M}\left[\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\frac{m(m-1)}{2}}\prod_{l=0}^{m-1}\left[\sum_{s=0}^{l}\binom{l}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{l-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^s\right]\right]} \tag{44}$$

$$\tilde{\pi}_{\beta,\beta\geq 1}^\infty \approx \frac{\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\frac{\beta(\beta-1)}{2}}\prod_{l=0}^{\beta-1}\left[\sum_{s=0}^{l}\binom{l}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{l-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^s\right]}{1+\sum_{m=1}^{M}\left[\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\frac{m(m-1)}{2}}\prod_{l=0}^{m-1}\left[\sum_{s=0}^{l}\binom{l}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{l-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^s\right]\right]} \tag{45}$$

$$\tilde{\pi}_{\beta}^{\infty} = \frac{\prod_{l=0}^{\beta-1} \frac{P^{\infty}(M)-P^{\infty}(M-l_1)P^{\infty}(M-l_2)}{1-P^{\infty}(l_1)P^{\infty}(l_2+1)}}{1+\sum_{m=1}^{M}\left[\prod_{l=0}^{m-1} \frac{P^{\infty}(M)-P^{\infty}(M-l_1)P^{\infty}(M-l_2)}{1-P^{\infty}(l_1)P^{\infty}(l_2+1)}\right]} \approx \frac{\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{\beta M}\left[\sum_{s=0}^{M}\binom{M}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]^{\beta}}{1+\sum_{m=1}^{M}\left[\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{mM}\left[\sum_{s=0}^{M}\binom{M}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M-s}\frac{(s+N_E-1)!}{(N_E-1)!}\bar{\gamma}_E^{s}\right]^{m}\right]} \tag{46}$$

APPENDIX C

According to [10], utilizing the asymptotic secrecy outage probability, the asymptotic stationary probability is given by, (46), as shown at the top of this page.

Due to the denominators in (46) has the term $1/\bar{\gamma}$, hence when $\bar{\gamma} \to \infty$ the corresponding term can be approximated as 0, and the desired results in **Corollary 2** can be easily obtained.

REFERENCES

[1] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[2] A. Host-Madsen and J. Zhang, "Capacity bounds and power allocation for wireless relay channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2020–2040, Jun. 2005.

[3] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[4] M. R. Bhatnagar, R. K. Mallik, and O. Tirkkonen, "Performance evaluation of best-path selection in a multihop decode-and-forward cooperative system," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2722–2728, Apr. 2016.

[5] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, "Buffering in a three-node relay network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[6] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.

[7] N. Zlatanov and R. Schober, "Buffer-aided relaying with adaptive link selection-fixed and mixed rate transmission," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2816–2840, May 2013.

[8] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, Mar. 2012.

[9] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

[10] P. Xu, Z. Ding, I. Krikidis, and X. Dai, "Achieving optimal diversity gain in buffer-aided relay networks with small buffer size," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8788–8794, Oct. 2016.

[11] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[12] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[14] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[15] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.

[16] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[17] L. Yang, M. O. Hasna, and I. S. Ansari, "Physical layer security for TAS/MRC systems with and without co-channel interference over η-μ fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12421–12426, Dec. 2018.

[18] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[19] J. Wan, D. Qiao, H.-M. Wang, and H. Qian, "Buffer-aided two-hop secure communications with power control and link selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635–7647, Nov. 2018.

[20] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[21] Y. Zhang, A. Sun, T. Liang, and X. Qiao, "Max-ratio relay selection for secure communication in amplify-and-forward buffer-aided cooperative networks," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Sep. 2015, pp. 1–4.

[22] A. Sun, T. Liang, and Y. Zhang, "Performance analysis of secure buffer-aided cognitive radio network," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Nov. 2015, pp. 1–4.

[23] X. Tang, Y. Cai, W. Yang, Y. Huang, T. Q. Duong, and W. Yang, "Secrecy outage analysis of buffer-aided multi-antenna relay systems without eavesdropper's CSI," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[24] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Vehi. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2018.

[25] X. Lu and R. C. de Lamare, "Relay selection based on the secrecy rate criterion for physical-layer security in buffer-aided relay networks," in *Proc. WSA 20th Int. ITG Workshop Smart Antennas*, Mar. 2016, pp. 1–5.

[26] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.

[27] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[28] Z. Tian, Y. Gong, G. Chen, and J. A. Chambers, "Buffer-aided relay selection with reduced packet delay in cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2567–2575, Mar. 2017.

[29] G. Chen, Y. Gong, P. Xiao, and R. Tafazolli, "Dual antenna selection in self-backhauling multiple small cell networks," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1611–1614, Aug. 2016.

[30] D. Chen, W. Yang, J. Hu, Y. Cai, and X. Tang, "Energy-efficient secure transmission design for the Internet of Things with an untrusted relay," *IEEE Access*, vol. 6, pp. 11862–11870, 2018.

[31] A. Afana, V. Asghari, A. Ghrayeb, and S. Affes, "Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints," in *Proc. IEEE 13th Int. Workshop Signal Process. Adv. Commun.*, Jun. 2012, pp. 429–433.